Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, therefore the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
ASP Fast Forum	A vulnerability has been reported in ASP Fast Forum that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	ASP Fast Forum Cross Site Scripting CVE-2005-3422	Medium	Secunia, Advisory: SA17387, October 31, 2005
Asus VideoSecurity Online 3.5	A vulnerability has been reported in VideoSecurity Online that could let remote malicious users traverse directories or disclose information. No workaround or patch available at time of publishing. There is no exploit code required.	Asus VideoSecurity Online Directory Traversal or Information Disclosure	Medium	Security Focus, ID: 15281, November 2, 2005

Comersus BackOffice	Multiple input validation vulnerabilities have been reported in BackOffice that could let remote malicious users disclose sensitive information, perform SQL injection, or conduct Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Comersus BackOffice Multiple Vulnerabilities CVE-2005-3397	Medium	Security Focus, ID: 15251, October 31, 2005
F-Secure Anti-Virus for Microsoft Exchange 6.40 and Internet Gatekeeper 6.40, 6.41, 6.42	A vulnerability has been reported in F-Secure Anti-Virus for Microsoft Exchange and Internet Gatekeeper that could let local malicious users traverse directories. Vendor fix available: http://www.f-secure.com/security/fsc-2005-2.shtml There is no exploit code required.	F-Secure Anti-Virus for Exchange and Internet Gatekeeper Directory Traversal CVE-2005-3468	Medium	Secunia, Advisory: SA17361, November 2, 2005
GraphOn GoGlobal for Windows prior to 3.1.0.3270	A buffer overflow vulnerability has been reported in GraphOn GoGlobal for Windows that could let a remote malicious user execute arbitrary code or cause a Denial of Service. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GraphOn GO-Global For Windows Denial of Service or Arbitrary Code Execution	High	Security Focus, ID: 15285, November 2, 2005
Hyper Estraier 1.0, 1.0.1	A vulnerability has been reported in Hyper Estraier that could let remote malicious users disclose information. Upgrade to version 1.0.2: http://hyperestraier.sourceforge.net/hyperestraier-1.0.2.tar.gz There is no exploit code required.	Hyper Estraier Information Disclosure CVE-2005-3421	Medium	Security Focus, ID: 15236, October 28, 2005
Microsoft Internet Explorer	A memory corruption vulnerability has been reported in Internet Explorer COM Object instantiation that could let remote malicious users execute arbitrary code.	Microsoft Internet Explorer Arbitrary Code Execution CVE-2005-1990	High	Microsoft Security Bulletin MS05-038, August 9, 2005 US-CERT VU#959049

	Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-038.mspx **V1.3 Issues discovered in in the security update: Microsoft Knowledge Base Article 906294.** A Proof of Concept exploit has been published.			**Microsoft Security Bulletin MS05-038 V1.3, November 2, 2005**
Microsoft Internet Explorer 5.01, 5.5, 6.0	A vulnerability has been reported in Internet Explorer that could let remote malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-052.mspx **V1.3 Issues discovered in in the security update: Microsoft Knowledge Base Article 909889.** Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf An exploit has been published.	Microsoft Internet Explorer Arbitrary Code Execution CVE-2005-2127	High	Microsoft, Security Bulletin MS05-052, October 11, 2005 Technical Cyber Security Alert TA05-284A, October 11, 2005 Avaya, ASA-2005-214, October 11, 2005 USCERT, VU#680526, VU#959049, VU#740372, VU#898241 **Microsoft, Security Bulletin MS05-052 V1.3, November 2, 2005**
Multiple Vendors Real Networks RealPlayer 10.5, v6.0.12.1053, v6.0.12.1040, 10.5 Beta v6.0.12.1016, 10.0 BETA, 10.0, v6.0.12.690, RealOne Player 2.0, 1.0; InnerMedia	A buffer overflow vulnerability has been reported in DynaZip that could let remote malicious users execute arbitrary code. RealPlayer/RealOne: Fixes are available via the "Check for Update" feature. DynaZip: Update to version 5.00.04 or later.	InnerMedia DynaZip Arbitrary Code Execution CVE-2004-1094	High	Security Focus, ID: 11555, October 27, 2005 US-CERT VU#582498

DynaZip Library 3.0 .0.14, 5.00.00-5.00.03; CheckMark Software Inc. MultiLedger 7.0, 6.0.3, CheckMark Payroll 3.9.1-3.9.6	DynaZip Max: Update to version 6.00.01 or later. CheckMark Software: http://www.checkmark.com/support/patch_win_pr.php An exploit has been published.			
RhinoSoft Serv-U FTP Server	A vulnerability has been reported in Serv-U FTP Server that could let remote malicious users cause a Denial of Service. Vendor upgrade available: http://www.serv-u.com/dn.asp There is no exploit code required.	Serv-U FTP Server Denial of Service CVE-2005-3467	Low	Secunia, Advisory: SA17409, November 2, 2005
RockLiffe Mailsite Express WebMail prior to 6.1.22	Multiple vulnerabilities have been reported in MailSite Express WebMail that could let remote malicious users disclose information, arbitrary file control, or execute arbitrary code. A vendor fix is available: http://www.rockliffe.com/userroom/download.asp There is no exploit code required.	RockLiffe MailSite Express WebMail Multiple Vulnerabilities CVE-2005-3428 CVE-2005-3429 CVE-2005-3430 CVE-2005-3431	Medium	Security Focus, ID: 15231, 15230, October 28, 2005
Techno Dreams Announcement, Guest Book, Mailing List, Web Directory	A vulnerability has been reported in Techno Dreams Announcement, Guest Book, Mailing List, and Web Directory that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Techno Dreams Multiple Product SQL Injection CVE-2005-3383 CVE-2005-3384 CVE-2005-3385 CVE-2005-3386	Medium	Secunia, Advisory: SA17354, October 27, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
Apple Apple Mac OS X Server 1-.4-10.4.2, Server	Multiple vulnerabilities have been reported: a misleading file ownership	Apple Mac OS X Security Update CVE-2005-2749	Medium	Apple Security Advisory, APPLE-SA-2005-10-31, October 31, 2005

10.3-10.3.9, 10.2-10.2.8, 10.0-10.1.5, Mac OS X 1-.4-10.4.2, 10.3-10.3.9, 10.2-10.2.8, 10.1-10.1.5, 10.0-10.0.4	display vulnerability was reported, which could result in a false sense of security; a software update failure vulnerability was reported, which could potentially result in a failure to install critical security fixes; a group membership alteration issue was reported, which could result in unauthorized access; an information disclosure vulnerability was reported in Keychain, which could let a malicious user obtain sensitive information; and multiple information disclosure vulnerabilities were reported in the kernel, which could potentially let malicious users obtain sensitive information. Update information available at: http://docs.info.apple.com/article.html?artnum=302763 Currently we are not aware of any exploits for these vulnerabilities.	CVE-2005-2750 CVE-2005-2751 CVE-2005-2739 CVE-2005-1126 CVE-2005-1406 CVE-2005-2752		
BeMoore Software News2Net 3.x	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'category' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	News2Net SQL Injection CVE-2005-3469	Medium	Secunia Advisory: SA17396, November 2, 2005
CVS CVS 1.12.7-1.12.12, 1.12.5, 1.12.2 , 1.12.1, 1.11.19, 1.11.17	A vulnerability has been reported in the 'cvsbug.in' script due to the insecure creation of temporary files,	CVS 'Cvsbug.In' Script Insecure Temporary File Creation	Low	Fedora Update Notifications FEDORA-2005-790 & 791, August 23, 2005

	which could let a malicious user cause data loss or a Denial of Service. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Trustix: http://http.trustix.org/pub/trustix/updates/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:20/cvsbug.patch SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Debian: http://security.debian.org/pool/updates/main/c/cvs/ http://security.debian.org/pool/updates/main/g/gcvs/ FreeBSD: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:20.cvsbug.asc **NetBSD:** **http://arkiv.netbsd.se/?ml=netbsd-announce&a=2005-10&m=1435804** There is no exploit code required.	CVE-2005-2693		Trustix Secure Linux Security Advisory, TSLSA-2005-0045, August 26, 2005 RedHat Security Advisory, RHSA-2005:756-3, September 6, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:20, September 7, 2005 Debian Security Advisories, DSA 802-1 & 806-1, September 7 & 9, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:20, September 9, 2005 **NetBSD Security Update, November 1, 2005**

FreeBSD IPSec AES-XCBC-MAC Algorithm V5.3, 5.4, 6.0Beta	A vulnerability has been reported in FreeBSD's IPSec AES-XCBC-MAC Algorithm, which could allow for incorrect key usage, and consequently allow remote malicious users to connect via unauthorized IPSec connections. A vendor patch is available: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:19/ **NetBSD:** **http://www.kame.net/dev/cvsweb2.cgi/kame/kame/sys/netinet6/ah_aesxcbcm ac.c.diff?r1=1.7&r2=1.8** There is no exploit code required.	FreeBSD IPSec AES-XCBC-MAC Algorithm Unauthorized Connections CVE-2005-2359	Medium	FreeBSD Security Advisory FreeBSD-SA-05:19, July 27, 2005 **Security Focus, Bugtraq ID: 14394, November 1, 2005**
IBM AIX 5.3 L, 5.3, 5.2.2, 5.2 L, 5.2, 5.1 L, 5.1	A buffer overflow vulnerability has been reported in the 'chcon' command. The impact was not specified Vendor patch available: http://www-03.ibm.com/servers/eserver/support/pseries/aixfixes.html Currently we are not aware of any exploits for this vulnerability.	IBM AIX 'chcon' Buffer Overflow CVE-2005-3396	Not Specified	IBM, IY78241, IY78253, October 28, 2005
Info-ZIP UnZip 5.52	A vulnerability has been reported due to a security weakness when extracting an archive to a world or group writeable directory, which could let a malicious user modify file permissions. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ SCO: ftp://ftp.sco.com/pub/	Info-ZIP UnZip File Permission Modification CVE-2005-2475	Medium	Security Focus, 14450, August 2, 2005 Fedora Update Notification, FEDORA-2005-844, September 9, 2005 SCO Security Advisory, SCOSA-2005.39, September 28, 2005 Ubuntu Security Notice, USN-191-1, September 29, 2005

	updates/OpenServer/ SCOSA-2005.39/507 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/u/unzip/ Trustix: http://http.trustix.org/pub/trustix/updates/ **Mandriva: http://www.mandriva.com/security/advisories** There is no exploit code required.			Trustix Secure Linux Security Advisory, TSLSA-2005-0053, September 30, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:197, October 26, 2005**
Luca Deri ntop 3.1	A vulnerability has been reported in 'ntopinitparms' due to the insecure creation of a temporary file, which could let a remote malicious user create/overwrite arbitrary files. Upgrade available at: http://prdownloads.sourceforge.net/ntop/ntop-3.2.tgz?download There is no exploit code required.	NTop Insecure Temporary File Creation CVE-2005-3387	Medium	Security Focus, Bugtraq ID: 15242, October 31, 2005
MailWatch for MailScanner MailWatch for MailScanner 1.0.2	Several vulnerabilities have been reported: an SQL injection vulnerability was reported due to insufficient sanitization of the 'authenticate()' function before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Directory Traversal vulnerability was reported in the ruleset view. The impact was not specified. Updates available at: http://sourceforge.net/project/showfiles.php?group_id=87163 There is no exploit code	MailWatch for MailScanner SQL Injection & Directory Traversal CVE-2005-3470 CVE-2005-3471	Medium	Secunia Advisory: SA17405, November 2, 2005

	required.			
Multiple Vendors Apache Mod_Auth_Shadow 1.0 to 1.4, 2.0	A vulnerability has been reported in Apache, Mod_Auth_Shadow, that could let remote malicious users bypass authentication. Upgrades available at: http://prdownloads.sourceforge.net/mod-auth-shadow/mod_auth_shadow-1.5 .tar.gz?download Debian: http://security.debian.org/pool/updates/main/m/mod-auth-shadow/ Mandriva: http://www.mandriva.com/security/advisories There is no exploit code required.	Apache Authentication Bypassing CVE-2005-2963	Medium	Security Focus, ID: 15224, October 27, 2005 Debian Security Advisory, DSA 844-1, October 5, 2005 Mandriva Linux Security Advisory MDKSA-2005:200, October 27, 2005
Multiple Vendors Linux Kernel Linux kernel 2.6- 2.6.14	A Denial of Service vulnerability has been reported in 'net/ipv6/udp.c' due to an infinite loop error in the 'udp_v6_get_port()' function. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Upgrades available at: http://kernel.org/pub/linux/kernel/v2.6/linux-2.6.14.tar.bz2** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IPV6 Denial of Service CVE-2005-2973	Low	Secunia Advisory: SA17261, October 21, 2005 Fedora Update Notifications, FEDORA-2005-1007 & 1013, October 20, 2005 **Security Focus, Bugtraq ID: 15156, October 31, 2005**

Multiple Vendors zlib 1.2.2, 1.2.1, 1.2 .0.7, 1.1-1.1.4, 1.0-1.0.9; Ubuntu Linux 5.0 4, powerpc, i386, amd64, 4.1 ppc, ia64, ia32; SuSE Open-Enterprise-Server 9.0, Novell Linux Desktop 9.0, Linux Professional 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Personal 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Enterprise Server 9; Gentoo Linux; FreeBSD 5.4, -RELENG, -RELEASE, -PRERELEASE, 5.3, -STABLE, -RELENG, -RELEASE; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; zsync 0.4, 0.3-0.3.3, 0.2-0.2.3, 0.1-0.1.6 1, 0.0.1-0.0.6	A buffer overflow vulnerability has been reported due to insufficient validation of input data prior to utilizing it in a memory copy operation, which could let a remote malicious user execute arbitrary code. Debian: ftp://security.debian.org/pool/updates/main/z/zlib/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:16/zlib.patch Gentoo: http://security.gentoo.org/glsa/glsa-200507-05.xml SUSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/ Mandriva: http://www.mandriva.com/security/advisories OpenBSD: http://www.openbsd.org/errata.html OpenPKG: ftp.openpkg.org RedHat: http://rhn.redhat.com/errata/RHSA-2005-569.html Trustix: http://http.trustix.org/pub/trustix/updates/ Slackware: ftp://ftp.slackware.com/pub/slackware/	Zlib Compression Library Buffer Overflow CVE-2005-2096	High	Debian Security Advisory DSA 740-1, July 6, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:16, July 6, 2005 Gentoo Linux Security Advisory, GLSA 200507-05, July 6, 2005 SUSE Security Announcement, SUSE-SA:2005:039, July 6, 2005 Ubuntu Security Notice, USN-148-1, July 06, 2005 RedHat Security Advisory, RHSA-2005:569-03, July 6, 2005 Fedora Update Notifications, FEDORA-2005-523, 524, July 7, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:11, July 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.013, July 7, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0034, July 8, 2005 Slackware Security Advisory, SSA:2005-189-01, July 11, 2005 Turbolinux Security Advisory, TLSA-2005-77,

	TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ zsync: http://prdownloads.sourceforge.net/zsync/zsync-0.4.1.tar.gz?download Apple: http://docs.info.apple.com/article.html?artnum=302163 SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33 IPCop: http://sourceforge.net/project/showfiles.php?group_id=40604&package_id = 35093&release_id=351848 Debian: http://security.debian.org/pool/updates/main/z/zsync/ Trolltech: ftp://ftp.trolltech.com/qt/source/qt-x11-free-3.3.5.tar.gz FedoraLegacy: http://download.fedoralegacy.org/fedora/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-18.xml Gentoo: http://security.gentoo.org/glsa/glsa-		July 11, 2005 Fedora Update Notification, FEDORA-2005-565, July 13, 2005 SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005 Security Focus, 14162, July 21, 2005 USCERT Vulnerability Note VU#680620, July 22, 2005 Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005 SCO Security Advisory, SCOSA-2005.33, August 19, 2005 Security Focus, Bugtraq ID: 14162, August 26, 2005 Debian Security Advisory, DSA 797-1, September 1, 2005 Security Focus, Bugtraq ID: 14162, September 12, 2005 Fedora Legacy Update Advisory, FLSA:162680, September 14, 2005 Gentoo Linux Security Advisory, GLSA 200509-18, September 26, 2005 Debian Security Advisory, DSA 797-2, September 29, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0055, October 7, 2005

	200509-18.xml Debian: http://security.debian.org/pool/updates/main/z/zsync/ Trustix: http://http.trustix.org/pub/trustix/updates/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101989-1 **Mandriva:** **http://www.mandriva.com/security/advisories** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/a/aide/** Currently we are not aware of any exploits for this vulnerability.			Sun(sm) Alert Notification Sun Alert ID: 101989, October 14, 2005 **Mandriva Linux Security Advisory MDKSA-2005:196, October 26, 2005** **Ubuntu Security Notice, USN-151-3, October 28, 2005**
Multiple Vendors zlib 1.2.2, 1.2.1; Ubuntu Linux 5.04 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Debian Linux 3.1 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A remote Denial of Service vulnerability has been reported due to a failure of the library to properly handle unexpected compression routine input. Zlib: http://www.zlib.net/zlib-1.2.3.tar.gz Debian: http://security.debian.org/pool/updates/main/z/zlib/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/ OpenBSD: http://www.openbsd.org/errata.html#libz2 Mandriva:	Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service CVE-2005-1849	Low	Security Focus, Bugtraq ID 14340, July 21, 2005 Debian Security Advisory DSA 763-1, July 21, 2005 Ubuntu Security Notice, USN-151-1, July 21, 2005 OpenBSD, Release Errata 3.7, July 21, 2005 Mandriva Security Advisory, MDKSA-2005:124, July 22, 2005 Secunia, Advisory: SA16195, July 25, 2005 Slackware Security Advisory, SSA:2005-203-03, July 22, 2005 FreeBSD Security

	http://www.mandriva.com/security/advisories?name=MDKSA-2005:124 Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.323596 FreeBSD: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:18.zlib.asc SUSE: http://lists.suse.com/archive/suse-security-announce/2005-Jul/0007.html Gentoo: http://security.gentoo.org/glsa/glsa-200507-28.xml http://security.gentoo.org/glsa/glsa-200508-01.xml Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Apple: http://docs.info.apple.com/article.html?artnum=302163 TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates/		Advisory, SA-05:18, July 27, 2005 SUSE Security Announcement, SUSE-SA:2005:043, July 28, 2005 Gentoo Linux Security Advisory, GLSA 200507-28, July 30, 2005 Gentoo Linux Security Advisory, GLSA 200508-01, August 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0040, August 5, 2005 Conectiva Linux Announcement, CLSA-2005:997, August 11, 2005 Apple Security Update, APPLE-SA-2005-08-15, August 15, 2005 Turbolinux Security Advisory, TLSA-2005-83, August 18, 2005 SCO Security Advisory, SCOSA-2005.33, August 19, 2005 Debian Security Advisory, DSA 797-1, September 1, 2005 Security Focus, Bugtraq ID: 14340, September 12, 2005 Fedora Legacy Update Advisory, FLSA:162680, September 14, 2005 Debian Security Advisory, DSA 797-2, September 29, 2005

	SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33 Debian: http://security.debian.org/pool/updates/main/z/zsync/ Trolltech: ftp://ftp.trolltech.com/qt/source/qt-x11-free-3.3.5.tar.gz FedoraLegacy: http://download.fedoralegacy.org/fedora/ Debian: http://security.debian.org/pool/updates/main/z/zsync/ **Mandriva:** **http://www.mandriva.com/security/advisories** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/a/aide/** Currently we are not aware of any exploits for this vulnerability.			**Mandriva Linux Security Advisory, MDKSA-2005:196, October 26, 2005** **Ubuntu Security Notice, USN-151-3, October 28, 2005**
Multiple Vendors Gentoo Linux; GNU GDB 6.3	Multiple vulnerabilities have been reported: a heap overflow vulnerability was reported when loading malformed object files, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported which could let a malicious user obtain elevated privileges. Gentoo: http://security.gentoo.org/glsa/glsa-200505-15.xml	GDB Multiple Vulnerabilities CVE-2005-1704 CVE-2005-1705	High	Gentoo Linux Security Advisory, GLSA 200505-15, May 20, 2005 Turbolinux Security Advisory, TLSA-2005-68, June 22, 2005 RedHat Security Advisory, RHSA-2005:659-9, September 28, 2005 RedHat Security Advisory, RHSA-2005:673-5 &

	Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gdb/ http://security.ubuntu.com/ubuntu/pool/main/b/binutils/ Mandriva: http://www.mandriva.com/security/advisories Trustix: http://http.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-659.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-673.html http://rhn.redhat.com/errata/RHSA-2005-709.html Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-222.pdf **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for these vulnerabilities.			RHSA-2005:709-6, October 5, 2005 Avaya Security Advisory, ASA-2005-222, October 18, 2005 **Fedora Update Notifications, FEDORA-2005-1032 & 1033, October 27, 2005**
Multiple Vendors Gnome-DB libgda 1.2.1; Debian Linux 3.1,	Format string vulnerabilities have been reported in 'gda-log.c' due to format string errors in the	GNOME-DB LibGDA Multiple Format String CVE-2005-2958	High	Security Focus, Bugtraq ID: 15200, October 25, 2005 Debian Security

sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	'gda_log_ error()' and 'gda_log_ message()' functions, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/libg/libgda2/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/libg/libgda2/** Currently we are not aware of any exploits for these vulnerabilities.			Advisory, DSA-871-1 & 871-2, October 25, 2005 **Ubuntu Security Notice, USN-212-1, October 28, 2005**
Multiple Vendors GNU gnump3d 2.9-2.9.5; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	A vulnerability has been reported in GNUMP3d that could let remote malicious users conduct Cross-Site Scripting or traverse directories. Upgrade to version 2.9.6: http://savannah.gnu.org/download/gnump3d/gnump3d-2.9.6.tar.gz Debian: http://security.debian.org/pool/updates/main/g/gnump3d/ There is no exploit code required; however, Proof of Concept exploits have been published.	GNUMP3d Cross-Site Scripting or Directory Traversal CVE-2005-3122 CVE-2005-3123	Medium	Security Focus Bugtraq IDs: 15226 & 15228, October 28, 2005 Debian Security Advisory DSA 877-1, October 28, 2005
Multiple Vendors Linux kernel 2.6-2.6.14	Several vulnerabilities have been reported: a Denial of Service vulnerability was reported due to a memory leak in '/security/keys/request_key_auth.c;' a Denial of Service vulnerability was reported due to a memory leak in '/fs/namei.c' when the 'CONFIG_AUDITSYSCALL' option is enabled; and a vulnerability was reported because the orinoco wireless driver fails to pad data packets with zeroes	Linux Kernel Denial of Service & Information Disclosure CVE-2005-3119 CVE-2005-3180 CVE-2005-3181	Medium	Secunia Advisory: SA17114, October 12, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0057, October 14, 2005 Fedora Update Notifications, FEDORA-2005-1013, October 20, 2005 **RedHat Security Advisory,**

	when increasing the length, which could let a malicious user obtain sensitive information. Patches available at: http://kernel.org/pub/linux/kernel/v2.6/testing/patch-2.6.14-rc4.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Trustix: http://http.trustix.org/pub/trustix/updates/ **RedHat: http://rhn.redhat.com/errata/RHSA-2005-808.html** There is no exploit code required.			**RHSA-2005:808-14, October 27, 2005**
Multiple Vendors Linux Kernel 2.6-2.6.14	Multiple vulnerabilities have been reported: a Denial of Service vulnerability was reported in the 'sys_set_mempolicy' function when a malicious user submits a negative first argument; a Denial of Service vulnerability was reported when threads are sharing memory mapping via 'CLONE_VM'; a Denial of Service vulnerability was reported in 'fs/exec.c' when one thread is tracing another thread that shares the same memory map; a Denial of Service vulnerability was reported in 'mm/ioremap.c' when performing a lookup of an non-existent page; a Denial of Service vulnerability was reported in the HFS and HFS+ (hfsplus) modules; and a remote Denial of Service vulnerability was reported due to a race condition in 'ebtables.c' when running on a SMP system that is operating	Multiple Vendors Linux Kernel Denials of Service CVE-2005-3053 CVE-2005-3106 CVE-2005-3107 CVE-2005-3108 CVE-2005-3109 CVE-2005-3110	Low	Ubuntu Security Notice, USN-199-1, October 10, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0057, October 14, 2005 **RedHat Security Advisory, RHSA-2005:808-14, October 27, 2005**

	under a heavy load. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Trustix: http://http.trustix.org/pub/trustix/updates/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-808.html** Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors RedHat Enterprise Linux WS 4, WS 3, 2.1, IA64, ES 4, ES 3, 2.1, IA64, AS 4, AS 3, AS 2.1, IA64, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1, IA64; OpenSSL Project OpenSSL 0.9.3-0.9.8, 0.9.2 b, 0.9.1 c; FreeBSD 6.0 -STABLE, -RELEASE, 5.4 -RELENG, -RELEASE, 5.3 -STABLE, -RELENG, -RELEASE, 5.3, 5.2.1 -RELEASE, -RELENG, 5.2 -RELEASE, 5.2, 5.1 -RELENG, -RELEASE/Alpha, 5.1 -RELEASE-p5, -RELEASE, 5.1, 5.0 -RELENG, 5.0, 4.11 -STABLE, -RELENG, 4.10 -RELENG, -RELEASE, 4.10	A vulnerability has been reported due to the implementation of the 'SSL_OP_MSIE_SSLV2_RSA_PADDING' option that maintains compatibility with third party software, which could let a remote malicious user bypass security. OpenSSL: http://www.openssl.org/source/openssl-0.9.7h.tar.gz FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:21/openssl.patch RedHat: http://rhn.redhat.com/errata/RHSA-2005-800.html Mandriva: http://www.mandriva.com/security/advisories Gentoo: http://security.gentoo.org/glsa/glsa-200510-11.xml Slackware:	Multiple Vendors OpenSSL Insecure Protocol Negotiation CVE-2005-2969	Medium	OpenSSL Security Advisory, October 11, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:21, October 11, 2005 RedHat Security Advisory, RHSA-2005:800-8, October 11, 2005 Mandriva Security Advisory, MDKSA-2005:179, October 11, 2005 Gentoo Linux Security Advisory, GLSA 200510-11, October 12, 2005 Slackware Security Advisory, SSA:2005-286-01, October 13, 2005 Fedora Update Notifications, FEDORA-2005-985 & 986, October 13, 2005 Sun(sm) Alert Notification Sun Alert ID: 101974, October 14, 2005

	ftp://ftp.slackware.com/pub/slackware/slackware Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101974-1 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/o/openssl/ OpenPKG: ftp://ftp.openpkg.org/release/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/trustix/updates/ SGI: http://www.sgi.com/support/security/ **Debian:** **http://security.debian.org/pool/updates/main/o/openssl094/** **NetBSD:** **http://arkiv.netbsd.se/?ml=netbsd-announce&a=2005-10&m=1435804** Currently we are not aware of any exploits for this vulnerability.			Ubuntu Security Notice, USN-204-1, October 14, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.022, October 17, 2005 SUSE Security Announcement, SUSE-SA:2005:061, October 19, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 SGI Security Advisory, 20051003-01-U, October 26, 2005 **Debian Security Advisory DSA 875-1, October 27, 2005** **NetBSD Security Update, November 1, 2005**
Multiple Vendors RedHat Fedora Core4, Core3, RedHat Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0;	A vulnerability has been reported in Pluggable Authentication Modules that could let local malicious users to bypass security restrictions.	Pluggable Authentication Modules Security Bypassing CVE-2005-2977	Medium	RedHat Security Advisory, RHSA-2005:805-6, October 26, 2005 Fedora Update Notifications

Linux-PAM Linux-PAM 0.77; Gentoo Linux	Redhat: https://rhn.redhat.com/errata/RHSA-2005-805.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200510-22.xml There is no exploit code required.			FEDORA-2005-1030 & 1031, October 27, 2005 Gentoo Linux Security Advisory, GLSA 200510-22, October 28, 2005
Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Netpbm 10.0	A buffer overflow vulnerability has been reported in the 'PNMToPNG' conversion package due to insufficient bounds checking of user-supplied input before coping to an insufficiently sized memory buffer, which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/netpbm-free/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-793.html Gentoo: http://security.gentoo.org/glsa/glsa-200510-18.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Mandriva: http://www.mandriva.com/security/advisories **Debian:** **http://security.debian.**	NetPBM Buffer Overflow CVE-2005-2978	High	Ubuntu Security Notice, USN-210-1, October 18, 2005 RedHat Security Advisory, RHSA-2005:793-6, October 18, 2005 Gentoo Linux Security Advisory, GLSA 200510-18, October 20, 2005 SUSE Security Summary Report, Announcement ID: SUSE-SR:2005:024, October 21, 2005 Mandriva Linux Security Advisory, MDKSA-2005:199, October 26, 2005 **Debian Security Advisory, DSA 878-1, October 28, 2005**

org/pool/updates/main/n/netpbm-free/

Currently we are not aware of any exploits for this vulnerability.

Multiple Vendors XFree86 X11R6 versions prior to 4.3.0; X.org X11R6 6.8.2; RedHat Enterprise Linux WS 2.1, IA64, ES 2.1, IA64, AS 2.1, IA64, Advanced Workstation for the Itanium Processor 2.1, IA64; Gentoo Linux	A buffer overflow vulnerability has been reported in the pixmap processing code, which could let a malicious user execute arbitrary code and possibly obtain superuser privileges. Gentoo: http://security.gentoo.org/glsa/glsa-200509-07.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-329.html http://rhn.redhat.com/errata/RHSA-2005-396.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/x/xfree86/ Mandriva: http://www.mandriva.com/security/advisories?name=MDKSA-2005:164 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Trustix: http://http.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/x/xfree86/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101926-1&searchclause SUSE: ftp://ftp.suse.com/pub/suse/ Slackware: ftp://ftp.slackware.com/	XFree86 Pixmap Allocation Buffer Overflow CVE-2005-2495	High	Gentoo Linux Security Advisory, GLSA 200509-07, September 12, 2005 RedHat Security Advisory, RHSA-2005:329-12 & RHSA-2005:396-9, September 12 & 13, 2005 Ubuntu Security Notice, USN-182-1, September 12, 2005 Mandriva Security Advisory, MDKSA-2005:164, September 13, 2005 US-CERT VU#102441 Fedora Update Notifications, FEDORA-2005-893 & 894, September 16, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005 Debian Security Advisory DSA 816-1, September 19, 2005 Sun(sm) Alert Notification Sun Alert ID: 101926, September 19, 2005 SUSE Security Announcement, SUSE-SA:2005:056, September 26, 2005 Slackware Security Advisory, SSA:2005-269-02, September 26, 2005 Sun(sm) Alert Notification Sun Alert ID: 101953, October 3, 2005

	pub/slackware/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101953-1 SUSE: ftp://ftp.SUSE.com/pub/SUSE Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-218.pdf Sun 101926: Updated Contributing Factors, Relief/Workaround, and Resolution sections. **NetBSD:** **http://arkiv.netbsd.se/?ml=netbsd-announce&a=2005-10&m=1435804** Currently we are not aware of any exploits for this vulnerability.			SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005 Avaya Security Advisory, ASA-2005-218, October 19, 2005 Sun(sm) Alert Notification Sun Alert ID: 101926, Updated October 24, 2005 **NetBSD Security Update, October 31, 2005**
OpenVPN OpenVPN 2.0-2.0.2	Several vulnerabilities have been reported: a format string vulnerability was reported in 'options.c' when handling command options in the 'foreign_option()' function, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability was reported due to a NULL pointer dereferencing error in the OpenVPN server when running in TCP mode. Updates available at: http://openvpn.net/download.html OpenPKG: ftp://ftp.openpkg.org/release/ Currently we are not aware of any exploits for these vulnerabilities.	OpenVPN Client Remote Format String & Denial of Service CVE-2005-3393	High	Secunia Advisory: SA17376, November 1, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.023, November 2, 2005

SCO UnixWare Portmapper	A vulnerability has been reported in UnixWare Portmapper that could let remote malicious users cause a Denial of Service. **SCO: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.43** Currently we are not aware of any exploits for this vulnerability.	UnixWare Portmapper Denial of Service CVE-2005-2132	Low	Security Focus, 14360, July 25, 2005 **SCO Security Advisory, SCOSA-2005.43, October 27, 2005**
Sun Microsystems, Inc. Sun Solaris 8, 9, 10	A vulnerability has been reported in Sun Solaris, Solaris Management Console, that could let local malicious users conduct Cross-Site Scripting. Vendor solution available: http://sunsolve.sun.com/search/document.do?assetkey=1-26-102016-1 There is no exploit code required.	Sun Solaris Cross-Site Scripting CVE-2005-3398	Medium	Sun, Alert ID: 102016, October 26, 2005
Sun Microsystems, Inc. Sun Java System Communications Express	A vulnerability has been reported due to an unspecified error that can be exploited by local/remote malicious users to obtain sensitive information. Patches available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101948-1 Currently we are not aware of any exploits for this vulnerability.	Sun Java System Communications Express Information Disclosure CVE-2005-3472	Medium	Sun(sm) Alert Notification Sun Alert ID: 101948, November 1, 2005
Sun Micro-systems, Inc. Solaris 10.0, 9.0 _x86, 9.0	A vulnerability has been reported in LD_AUDIT,' which could let a malicious user obtain superuser privileges. Workaround and patch	Sun Solaris Runtime Linker 'LD_AUDIT' Elevated Privileges CVE-2005-2072	High	Security Focus, 14074, June 28, 2005 Sun(sm) Alert Notification, 101794, June 28, 2005 Sun(sm) Alert

	information available at: **http://sunsolve.sun.com/search/document.do?assetkey=1-26-101794-1** Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-162.pdf An exploit script has been published.			Notification, 101794, Updated July 12, 13, 15, 2005 Avaya Security Advisory, ASA-2005-162, August 2, 2005 **Sun(sm) Alert Notification, 101794, Updated October 31, 2005**
Todd Miller Sudo 1.x	A vulnerability has been reported in the environment cleaning due to insufficient sanitization, which could let a malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/s/sudo/ **Mandriva:** **http://www.mandriva.com/security/advisories** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/s/sudo/** There is no exploit code required.	Todd Miller Sudo Local Elevated Privileges CVE-2005-2959	Medium	Debian Security Advisory, DSA 870-1, October 25, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:201, October 27, 2005** **Ubuntu Security Notice, USN-213-1, October 28, 2005**
Uim Uim 0.5 .0, 0.4.9	A vulnerability has been reported in 'uim/uim-custom.c' due to the incorrect use of several environment variables, which could let a malicious user obtain elevated privileges. Updates available at: http://uim.freedesktop.org/releases/uim-0.4.9.1.tar.gz **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code	Uim Elevated Privileges CVE-2005-3149	Medium	Secunia Advisory: SA17043, October 4, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:198, October 26, 2005**

	required.			
xloadimage xloadimage 4.1 and earlier	A buffer overflow vulnerability has been reported when handling the title of a NIFF image when performing zoom, reduce, or rotate functions, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/x/xloadimage/ http://security.debian.org/pool/updates/main/x/xli/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-802.html **Mandriva: http://www.mandriva.com/security/advisories** SUSE: ftp://ftp.SUSE.com/pub/SUSE SGI: http://www.sgi.com/support/security/ **Gentoo: http://security.gentoo.org** Currently we are not aware of any exploits for this vulnerability.	Xloadimage NIFF Image Buffer Overflow CVE-2005-3178	High	Debian Security Advisories, DSA 858-1 & 859-1, October 10, 2005 RedHat Security Advisory, RHSA-2005:802-4, October 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:191, October 21, 2005 SUSE Security Summary Report, SUSE-SR:2005:024, October 21, 2005 SGI Security Advisory, 20051003-01-U, October 26, 2005 **Gentoo Linux Security Advisory, GLSA 200510-26, October 31, 2005**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
Alexander Palmo Simple PHP Blog 0.4.5 & prior	Cross-Site Scripting vulnerabilities have been reported in 'preview_cgi.php' and 'preview_static_cgi.php'	Simple PHP Blog Cross-Site Scripting	Medium	Technical University of Vienna Security Advisory TUVSA-0511-001,

	due to insufficient sanitization of the 'entry parameter, in preview_cgi.php' due to insufficient sanitization of the 'blog_subject' and 'blog_text' parameters, in 'preview_static_cgi.php' due to insufficient sanitization of the 'blog_ subject,' 'blog_text,' and 'file_name' parameters, and in 'colors_cgi.php' due to insufficient sanitization of the 'scheme_name' and the 'bg_color' parameters, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	CVE-2005-3473		November 2, 2005
ATutor ATutor 1.5.1-pl1, 1.5.1, 1.4.1-1.4.3 ATutor	Multiple vulnerabilities have been reported in ATutor that could let remote malicious users conduct Cross-Site Scripting, disclose sensitive information, or execute arbitrary code. Vendor patch available: http://atutor.ca/view/3/6158/1.html There is no exploit code required; however, Proof of Concept exploits have been published.	ATutor Multiple Vulnerabilities	High	Secunia, Advisory: SA16915, October 27, 2005
Cisco Systems CiscoWorks Management Center for IPS Sensors (IPSMC) 2.1	A vulnerability has been reported due to an error in the Cisco IOS IPS (Intrusion Prevention System) configuration file that is generated by the IPS MC and deployed to IOS IPS devices, which could potentially allow malicious traffic to pass through. Patch information available at: http://www.cisco.com/warp/public/707/cisco-sa-20051101-ipsmc.shtml	Cisco Management Center for IPS Sensors Signature Disable CVE-2005-3427	Medium	Cisco Security Advisory, 68065, November 1, 2005 US-CERT VU#154883

	There is no exploit code required.			
codetosell. com ViArt Shop Enterprise 2.x	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in the 'basket.php,' 'forum.php,' 'page.php,' 'reviews.php,' 'products.php,' and 'news_view.php' scripts due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-SIte Scripting vulnerability was reported in the 'forum_new_ thread.php' script due to insufficient sanitization of input passed to the nickname, email, topic and message fields and the nickname and message fields in 'forum_threads.php,' which could let a remote malicious user execute arbitrary HTML and script code. **ViArt Shop Enterprise 2.1.8 & later versions are not affected by these issues. Please contact the vendor to obtain a fixed version.** There is no exploit code required; however, Proofs of Concepts have been published.	ViArt Shop Enterprise Cross-Site Scripting CVE-2005-1440	High	Secunia Advisory, SA15181, May 2, 2005 **Security Focus, Bugtraq ID: 13462, October 27, 2005**

eyeOS eyeOS 0.8.4 -r1, 0.8.4, 0.8.3 -r2, 0.8.3	Several vulnerabilities have been reported: a vulnerability was reported in 'desktop.php' due to insufficient sanitization of the 'motd' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported because user credentials are stored in the file 'usrinfo.xml' inside the web root, which could let a remote malicious user obtain sensitive information. Update available at: http://www.eyeos.org/?section=Downloads There is no exploit code required.	eyeOS Script Insertion & Information Disclosure CVE-2005-3413 CVE-2005-3414	Medium	Secunia Advisory: SA17105, November 1, 2005
First4Internet Ltd. XCP Content Management	A vulnerability has been reported in 'aries.sys' due to the device driver hiding all files, registry keys and processes on the system that have names that start with "sys", which could let a malicious user bypass security. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	First4Internet XCP Content Management Security Bypass CVE-2005-3474	Medium	Secunia Advisory: SA17408, November 2, 2005
gCards gCards 1.44	An SQL injection vulnerability has been reported in 'news.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	gCards SQL Injection CVE-2005-3408	Medium	Security Tracker, Alert ID: 1015106, October 25, 2005
Hasbani Hasbani Web Server	A vulnerability has been reported in Hasbani Web Server that could let remote malicious users cause a Denial	Hasbani Web Server Denial of Service CVE-2005-3475	Low	Security Focus, ID: 15225, October 27, 2005

	of Service. No workaround or patch available at time of publishing. An exploit has been published.			
Hewlett Packard Company OpenVMS Integrity 8.2-1, 8.2, OpenVMS Alpha 7.3-2, 8.2	A Denial of Service vulnerability has been reported due to an unspecified error. Patch available at: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBOV01239 Currently we are not aware of any exploits for this vulnerability.	HP OpenVMS Denial of Service CVE-2005-3476	Low	HP Security Bulletin, HPSBOV01239, October 31, 2005
Invision Power Services Invision Gallery 2.0.3	A vulnerability has been reported in the image upload handling due to an input validation error, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Invision Gallery Image Input Validation CVE-2005-3477	Medium	Secunia Advisory: SA17393, November 2, 2005
Invision Power Services Invision Gallery 2.0.3	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the the 'st' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Invision Gallery SQL Injection CVE-2005-3395	Medium	Secunia Advisory: SA17375, November 1, 2005
Jed Wing CHM lib 0.35, 0.3- 0.33, 0.2, 0.1	A buffer overflow vulnerability has been reported in '_chm_find_in_PMGL' due to a failure to properly bounds check input data prior to copying it into an insufficiently sized memory buffer, which could let a remote malicious user execute	Jed Wing CHM Lib '_chm_find_in_PMG'L Remote Buffer Overflow CVE-2005-2930	High	iDefense Security Advisory, October 28, 2005

	arbitrary code. Upgrades available at: http://morte.jedrea.com/~jedwin/projects/chmlib/chmlib-0.36.tgz Currently we are not aware of any exploits for this vulnerability.			
Mantis Mantis 1.0.0RC2, 0.19.2	Several vulnerabilities have been reported: a vulnerability was reported in 'bug_sponsorship_list_view_inc.php' due to insufficient verification before used to include files, which could let a remote malicious user execute arbitrary files; an SQL injection vulnerability was reported due to insufficient sanitization of unspecified input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; several Cross-Site Scripting vulnerabilities were reported in JavaScript and 'mantis/view_all_set.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; an unspecified vulnerability was reported when using reminders, which could lead to the disclosure of sensitive information; and a vulnerability was reported because the User ID is cached longer than necessary. Upgrades available at: http://prdownloads.sourceforge.net/mantisbt/mantis-0.19.3.tar.gz **Gentoo:** **http://security.gentoo.org/glsa/glsa-200510-24.xml** There is no exploit code required; however, Proof of Concept exploits have been published.	Mantis Multiple Vulnerabilities CVE-2005-3335 CVE-2005-3336 CVE-2005-3337 CVE-2005-3338 CVE-2005-3339	High	Secunia Advisory: SA16818, October 26, 2005 **Gentoo Linux Security Advisory, GLSA 200510-24, October 28, 2005**
Multiple Vendors ALT Linux	Two buffer overflow vulnerabilities have been	Telnet Client 'slc_add_reply()'	High	iDEFENSE Security Advisory,

Compact 2.3, Junior 2.3; Apple Mac OS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8, Mac OS X Server 10.0, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8; MIT Kerberos 5 1.0, 5 1.0.6, 5 1.0.8, 51.1-5 1.4; Netkit Linux Netkit 0.9-0.12, 0.14-0.17, 0.17.17; Openwall GNU/*/Linux (Owl)-current, 1.0, 1.1; FreeBSD 4.10-PRERELEASE, 2.0, 4.0 .x, -RELENG, alpha, 4.0, 4.1, 4.1.1 -STABLE, -RELEASE, 4.1.1, 4.2, -STABLE pre122300, -STABLE pre050201, 4.2 -STABLE, -RELEASE, 4.2, 4.3 -STABLE, -RELENG, 4.3 -RELEASE -p38, 4.3 -RELEASE, 4.3, 4.4 -STABLE, -RELENG, -RELEASE-p42, 4.4, 4.5 -STABLE pre2002-03-07, 4.5 -STABLE, -RELENG, 4.5 -RELEASE-p32, 4.5 -RELEASE, 4.5, 4.6 -STABLE, -RELENG, 4.6 -RELEASE -p20, 4.6 -RELEASE, 4.6, 4.6.2, 4.7 -STABLE, 4.7 -RELENG, 4.7 -RELEASE-p17, 4.7 -RELEASE, 4.7, 4.8	reported in Telnet: a buffer overflow vulnerability has been reported in the 'slc_add_reply()' function when a large number of specially crafted LINEMODE Set Local Character (SLC) commands is submitted, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported in the 'env_opt_add()' function, which could let a remote malicious user execute arbitrary code. ALTLinux: http://lists.altlinux.ru/pipermail /security-announce/2005-March/000287.html Apple: http://wsidecar.apple.com/cgi-bin/ nph-reg3rdpty1.pl/product=05529& platform=osx&method=sa/SecUpd 2005-003Pan.dmg Debian: http://security.debian.org/pool/ updates/main/n/netkit-telnet/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:01/ MIT Kerberos: http://web.mit.edu/kerberos/advisories/2005-001-patch_1.4.txt Netkit: ftp://ftp.uk.linux.org/pub/linux/Networking/netkit/ Openwall: http://www.openwall.com/Owl/ CHANGES-current.shtml	& 'env_opt_add()' Buffer Overflows CVE-2005-0468 CVE-2005-0469		March 28, 2005 US-CERT VU#291924 Mandrakelinux Security Update Advisory, MDKSA-2005:061, March 30, 2005 Gentoo Linux Security Advisories, GLSA 200503-36 & GLSA 200504-01, March 31 & April 1, 2005 Debian Security Advisory, DSA 703-1, April 1, 2005 US-CERT VU#341908 Gentoo Linux Security Advisory, GLSA 200504-04, April 6, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 Sun(sm) Alert Notification, 57761, April 7, 2005 SCO Security Advisory, SCOSA-2005.21, April 8, 2005 Avaya Security Advisory, ASA-2005-088, April 27, 2005 Gentoo Linux Security Advisory, GLSA 200504-28, April 28, 2005 Turbolinux Security Advisory, TLSA-2005-52, April 28, 2005

-RELENG, 4.8 -RELEASE-p7, 4.8 -PRE RELEASE, 4.8, 4.9 -RELENG, 4.9 -PRE RELEASE, 4.9, 4.10 -RELENG, 4.10 -RELEASE, 4.10, 4.11 -STABLE, 5.0 -RELENG, 5.0, 5.1 -RELENG, 5.1 -RELEASE-p5, 5.1 -RELEASE, 5.1, 5.2 -RELENG, 5.2 -RELEASE, 5.2, 5.2.1 -RELEASE, 5.3 -STABLE, 5.3 -RELEASE, 5.3, 5.4 -PRE RELEASE; SuSE Linux 7.0, sparc, ppc, i386, alpha, 7.1, x86, sparc, ppc, alpha, 7.2, i386; SGI IRIX 6.5.24-6.5.27	RedHat: http://rhn.redhat.com/errata/ RHSA-2005-327.html Sun: http://sunsolve.sun.com/ search/ document.do? assetkey= 1-26-57755-1 SUSE: ftp://ftp.SUSE.com/ pub/SUSE Ubuntu: http://security.ubuntu.com/ ubuntu/ pool/main/n/ netkit-telnet/ OpenBSD: http://www.openbsd.org/ errata.html#telnet Mandrake: http://www.mandrakesecure .net/ en/ftp.php Gentoo: http://security.gentoo.org/ glsa/glsa-200503-36.xml http://security.gentoo.org/ glsa/glsa-200504-01.xml Debian: http://security.debian.org/ pool/updates/main/k/krb5/ Gentoo: http://security.gentoo.org/ glsa/glsa-200504-04.xml SGI: ftp://oss.sgi.com/projects/ sgi_propack/download /3/updates/ SCO: ftp://ftp.sco.com/pub/ updates/ UnixWare/ SCOSA-2005.21 Sun: http://sunsolve.sun.com/ search/document.do? assetkey=1-26-57761-1 Openwall:		Sun(sm) Alert Notification, 57761, April 29, 2005 SCO Security Advisory, SCOSA-2005.23, May 17, 2005 SGI Security Advisory, 20050405-01-P, May 26, 2005 Debian Security Advisory, DSA 731-1, June 2, 2005 Conectiva Security Advisory, CLSA-2005:962, June 6, 2005 Trustix Secure Linux Security Advisory, TLSA-2005-0028, June 13, 2005 Avaya Security Advisory, ASA-2005-132, June 14, 2005 Fedora Legacy Update Advisory, FLSA:152583, July 11, 2005 Slackware Security Advisory, SSA:2005-210-01, August 1, 2005 Debian Security Advisory, DSA 773-1, August 11, 2005 **Security Focus, Bugtraq ID: 12919, November 1, 2005**

	http://www.openwall.com/Owl/CHANGES-current.shtml Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-088_RHSA-2005-330.pdf Gentoo: http://security.gentoo.org/glsa/glsa-200504-28.xml TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Sun: http://sunsolve.sun.com/search/ document.do?assetkey=1-26-57761-1 OpenWall: http://www.openwall.com/Owl/CHANGES-current.shtml SCO: ftp://ftp.sco.com/pub/updates/ OpenServer/SCOSA-2005.23 SGI IRIX: Apply patch 5892 for IRIX 6.5.24-6.5.27: ftp://patches.sgi.com/support/free/security/patches/ Debian: http://security.debian.org/pool/updates/main/k/krb4/ Conectiva: http://distro.conectiva.com.br/ atualizacoes/index.php?id=a&anuncio=000962 Trustix: ftp://ftp.trustix.org/pub/trustix/ updates/ Avaya: http://support.avaya.com/	

elmodocs2/security/ASA-2005-132_RHSA-2005-327.pdf

FedoraLegacy:
http://download.fedoralegacy.org/redhat/

Slackware:
ftp://ftp.slackware.com/pub/slackware/

Debian:
http://security.debian.org/pool/updates/main/

NetBSD 2.0.3 is not vulnerable to this issue. Please contact the vendor for more information.

Currently we are not aware of any exploits for these vulnerabilities.

Multiple Vendors Concurrent Versions System (CVS) 1.x;Gentoo Linux; SuSE Linux 8.2, 9.0, 9.1, x86_64, 9.2, x86_64, 9.3, Linux Enterprise Server 9, 8, Open-Enterprise-Server 9.0, School-Server 1.0, SUSE CORE 9 for x86, UnitedLinux 1.0	Multiple vulnerabilities have been reported: a buffer overflow vulnerability was reported due to an unspecified boundary error, which could let a remote malicious user potentially execute arbitrary code; a remote Denial of Service vulnerability was reported due to memory leaks and NULL pointer dereferences; an unspecified error was reported due to an arbitrary free (the impact was not specified), and several errors were reported in the contributed Perl scripts, which could let a remote malicious user execute arbitrary code. Update available at: https://ccvs.cvshome.org/servlets/ProjectDocumentList Gentoo: http://security.gentoo.org/glsa/glsa-200504-16.xml SuSE: ftp://ftp.suse.com/pub/suse/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ FreeBSD: ftp://ftp.FreeBSD.org/pub/ Peachtree: http://peachtree.burdell.org/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-387.html	CVS Multiple Vulnerabilities CVE-2005-0753	High	Gentoo Linux Security Advisory, GLSA 200504-16, April 18, 2005 SuSE Security Announcement, SUSE-SA:2005:024, April 18, 2005 Secunia Advisory, SA14976, April 19, 2005 Fedora Update Notification, FEDORA-2005-330, April 20, 2006 Mandriva Linux Security Update Advisory, MDKSA-2005:073, April 21, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0013, April 21, 2005 Gentoo Linux Security Advisory [UPDATE], GLSA 200504-16:02, April 22, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:05, April 22, 2005 Peachtree Linux Security Notice, PLSN-0005, April 22, 2005 RedHat Security Advisory, RHSA-2005:387-06, April 25, 2005 Turbolinux Security Advisory, TLSA-2005-51, April 28, 2005 Ubuntu Security Notice, USN-117-1

	OpenBSD: http://www.openbsd.org/errata.html#cvs TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ OpenBSD: http://www.openbsd.org/errata35.html# Ubuntu: http://security.ubuntu.com/Subunit/pool/main/c/cvs/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ OpenBSD: http://www.openbsd.org/errata.html#cvs Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000966 Debian: http://security.debian.org/pool/ updates/main **NetBSD:** **http://www.NetBSD.org/** Currently we are not aware of any exploits for these vulnerabilities.		May 04, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 Conectiva Security Advisory, CLSA-2005:966, June 13, 2005 Debian Security Advisory, DSA 773-1, August 11, 2005 **NetBSD Security Update, November 1, 2005**

Multiple Vendors
MandrakeSoft Linux Mandrake 2006.0 x86_64, 2006.0, 10.2 x86_64, 10.2;
Gentoo Linux;
Ethereal Group Ethereal 0.10.1-0.10.13, 0.9-0.9.16, 0.8.19, 0.8.18, 0.8.13-0.8.15, 0.8.5, 0.8, 0.7.7
	A vulnerability has been reported in Ethereal, IRC Protocol Dissector, that could let remote malicious users cause a Denial of Service.
	Mandriva: http://www.mandriva.com/security/advisories
	Gentoo: http://security.gentoo.org/glsa/glsa-200510-25.xml
	Currently we are not aware of any exploits for this vulnerability.
		Ethereal Denial of Service
		CVE-2005-3313
			Low	Mandriva Linux Security Advisory, MDKSA-2005:193-1, October 26, 2005
				Gentoo Linux Security Advisor, GLSA 200510-25, October 30, 2005

Multiple Vendors RedHat Fedora Core4, Core3; Ethereal Group Ethereal 0.10 -0.10.12, 0.9-0.9.16, 0.8.19, 0.8.18	Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported in the ISAKMP, FC-FCS, RSVP, and ISIS LSP dissectors; a remote Denial of Service vulnerability was reported in the IrDA dissector; a buffer overflow vulnerability was reported in the SLIMP3, AgentX, and SRVLOC dissectors, which could let a remote malicious user execute arbitrary code; a remote Denial of Service vulnerability was reported in the BER dissector; a remote Denial of Service vulnerability was reported in the SigComp UDVM dissector; a remote Denial of service vulnerability was reported due to a null pointer dereference in the SCSI, sFlow, and RTnet dissectors; a vulnerability was reported because a remote malicious user can trigger a divide by zero error in the X11 dissector; a vulnerability was reported because a remote malicious user can cause an invalid pointer to be freed in the WSP dissector; a remote Denial of Service vulnerability was reported if the 'Dissect unknown RPC program numbers' option is enabled (not the default setting); and a remote Denial of Service vulnerability was reported if	Ethereal Multiple Protocol Dissector Vulnerabilities CVE-2005-3184 CVE-2005-3241 CVE-2005-3242 CVE-2005-3243 CVE-2005-3244 CVE-2005-3245 CVE-2005-3246 CVE-2005-3247 CVE-2005-3248 CVE-2005-3249	High	Ethereal Security Advisory, enpa-sa-00021, October 19, 2005 Fedora Update Notifications, FEDORA-2005-1008 & 1011, October 20, 2005 RedHat Security Advisory, RHSA-2005:809-6, October 25, 2005 Mandriva Linux Security Advisory, MDKSA-2005:193, October 25, 2005 **Avaya Security Advisory, ASA-2005-227, October 28, 2005** **Gentoo Linux Security Advisory, GLSA 200510-25, October 30, 2005** **Mandriva Linux Security Advisory, MDKSA-2005:193-2, October 31, 2005**

	SMB transaction payload reassembly is enabled (not the default setting). Upgrades available at: http://prdownloads.sourceforge.net/ethereal/ethereal-0.10.13.tar.gz?download Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-809.html **Mandriva: http://www.mandriva.com/security/advisories** **Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-227.pdf** **Gentoo: http://security.gentoo.org/glsa/glsa-200510-25.xml** An exploit script has been published.			
Multiple Vendors Ukranian National Antivirus UNA; Trend Micro PC-cillin 2005, OfficeScan Corporate Edition 7.0; Sophos Anti-Virus 3.91; Panda Titanium Norman Virus Control 5.81; McAfee Internet Security Suite 7.1.5; Kaspersky Labs Anti-Virus 5.0.372; Ikarus Ikarus 2.32; F-Prot Antivirus 3.16 c; eTrust CA 7.0.14; Dr.Web 4.32 b; AVG Anti-Virus 7.0.323; ArcaBit ArcaVir 2005.0	A vulnerability has been reported in the scanning engine routine that determines the file type if the MAGIC BYTE of the EXE files is at the beginning, which could lead to a false sense of security and arbitrary code execution. **The following software titles/versions are not affected by this issue:** VirusBlokAda VBA32 Trend Micro PC-cillin 2006 Symantec Norton Internet Security 2005 11.5.6 .14 Symantec AntiVirus Corporate Edition 10.0 Sophos Anti-Virus 5.0.2 Sophos Anti-Virus 3.95	Multiple Vendors Anti-Virus Magic Byte Detection Evasion CVE-2005-3370 CVE-2005-3371 CVE-2005-3372 CVE-2005-3373 CVE-2005-3374 CVE-2005-3375 CVE-2005-3376 CVE-2005-3377 CVE-2005-3378 CVE-2005-3379 CVE-2005-3380 CVE-2005-3381 CVE-2005-3382 CVE-2005-3399	High	Security Focus, Bugtraq ID: 15189, October 25, 2005 **Security Focus, Bugtraq ID: 15189, October 31, 2005**

	Softwin BitDefender 8.0 NOD32 NOD32 2.50.25 H+BEDV AntiVir Personal 6.31 .00.01 F-Secure Anti-Virus 5.56 ClamWin ClamWin 0.86.1 Avast! Antivirus Home Edition 4.6.655 **Please contact the vendor to obtain fixes.** A Proof of Concept exploit has been published.	CVE-2005-3400 CVE-2005-3401	

Multiple Vendors University of Kansas Lynx 2.8.6 dev.1-dev.13, 2.8.5 dev.8, 2.8.5 dev.2-dev.5, 2.8.5, 2.8.4 rel.1, 2.8.4, 2.8.3 rel.1, 2.8.3 pre.5, 2.8.3 dev2x, 2.8.3 dev.22, 2.8.3, 2.8.2 rel.1, 2.8.1, 2.8, 2.7; RedHat Enterprise Linux WS 4, WS 3, 2.1, ES 4, ES 3, ES 2.1, AS 4, AS 3, AS 2.1, RedHat Desktop 4.0, 3.0, RedHat Advanced Workstation for the Itanium Processor 2.1 IA64	A buffer overflow vulnerability has been reported in the 'HTrjis()' function in the Lynx application when handling NNTP article headers, which could let a remote malicious user execute arbitrary code. University of Kansas Lynx: http://lynx.isc.org/current/lynx2.8.6dev.14.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200510-15.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lynx/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-803.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Trustix: http://http.trustix.org/pub/trustix/updates/ SGI: http://www.sgi.com/support/security/ Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/l/lynx/ http://security.debian.	Lynx 'HTrjis()' NNTP Remote Buffer Overflow CVE-2005-3120	High	Gentoo Linux Security Advisory, GLSA 200510-15, October 17, 2005 Ubuntu Security Notice, USN-206-1, October 17, 2005 RedHat Security Advisory, RHSA-2005:803-4, October 17, 2005 Fedora Update Notifications, FEDORA-2005-993 & 994, October 17, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:186, October 18, 2005 Conectiva Linux Announcement, CLSA-2005:1037, October 19, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 SGI Security Advisory, 20051003-01-U, October 26, 2005 Mandriva Linux Security Advisory, MDKSA-2005:186-1, October 26, 2005 Debian Security Advisories, DSA 874-1 & 876-1, October 27, 2005 **Ubuntu Security Notice, USN-206-2, October 29, 2005**

	org/pool/updates/main/l/lynx-ssl/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/l/lynx/** **(Note: Ubuntu advisory USN-206-1 was previously released to address this vulnerability, however, the fixes contained an error that caused lynx to crash.)** A Proof of Concept Denial of Service exploit script has been published.			
Novell ZENworks Patch Management 6.0.0.52	A vulnerability has been reported in ZENworks Patch Management that could let local malicious users perform SQL injection. Upgrade to version 6.2.2.181: http://download.novell.com There is no exploit code required; however, Proof of Concept exploits have been published.	Novell ZENworks Patch Management SQL Injection CVE-2005-3315	Medium	Novell, TID10099318, October 27, 2005
OaBoard OaBoard 1.0	An SQL injection vulnerability has been reported in 'forum.php' due to insufficient sanitization of the 'channel' and 'topic' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	OaBoard SQL Injection CVE-2005-3394	Medium	Secunia Advisory: SA17373, November 1, 2005
PBLang PBLang 4.65	Multiple vulnerabilities have been reported in PBLang that could let remote malicious users conduct Cross-Site Scripting or execute arbitrary code. No workaround or patch available at time of publishing.	PBLang Multiple Cross-Site Scripting Vulnerabilities	High	Security Focus, ID: 15223, October 27, 2005

	There is no exploit code required; however, Proof of Concept exploits have been published.			
PHP Advanced Transfer Manager PHP Advanced Transfer Manager 1.30	A vulnerability has been reported in PHP Advanced Transfer Manager that could let remote malicious users obtain unauthorized access. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	PHP Advanced Transfer Manager Unauthorized Access	Medium	Security Focus, ID: 15237, October 29, 2005
PHP Group PHP 5.0.5, 4.4.0	A vulnerability has been reported in the 'open_basedir' directive due to the way PHP handles it, which could let a remote malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Trustix: http://http.trustix.org/pub/trustix/updates/ **Upgrades available at:** **http://www.php.net/** There is no exploit code required.	PHP 'Open_BaseDir' Information Disclosure CVE-2005-3054	Medium	Security Focus, Bugtraq ID: 14957, September 27, 2005 Ubuntu Security Notice, USN-207-1, October 17, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 **Security Focus, Bugtraq ID: 14957, October 31, 2005**
PHP PHP 4.0.x, 4.1.x, 4.2.x, 4.3.x, 4.4.x, 5.0.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to insufficient protection of the 'GLOBALS' array, which could let a remote malicious user define global variables; a vulnerability was reported in the 'parse_str()' PHP function when handling an unexpected termination, which could let a remote malicious user enable the 'register_ globals' directive; a Cross-Site Scripting vulnerability was reported in the 'phpinfo()' PHP function due to insufficient sanitization of user-supplied	PHP Multiple Vulnerabilities CVE-2005-3388 CVE-2005-3389 CVE-2005-3390 CVE-2005-3391 CVE-2005-3392	Medium	Secunia Advisory: SA17371, October 31, 2005

	input, which could let a remote malicious user execute arbitrary HTML and script code; and an integer overflow vulnerability was reported in 'pcrelib' due to an error, which could let a remote malicious user corrupt memory. Upgrades available at: http://www.php.net/get/php-4.4.1.tar.gz There is no exploit code required.			
phpBB Group phpBB 2.0.17 & prior	Multiple vulnerabilities have been reported due to improper deregistration of global variables, which could let a remote malicious user conduct Cross-Site Scripting, execute arbitrary PHP code, or perform SQL injection. Upgrades available at: http://www.phpbb.com/files/releases/phpbb_2.0.17_to_2.0.18.zip There is no exploit code required.	phpBB Deregistration Global Variables CVE-2005-3415	Medium	Security Focus, Bugtraq ID: 15243, October 31, 2005
PHPCafe Tutorial Manager PHPCafe Tutorial Manager	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPCafe Tutorial Manager SQL Injection CVE-2005-3478	Medium	Security Focus, Bugtraq ID: 15244, October 31, 2005
phpESP phpESP 1.7.5, -dev3, -dev2, -dev	A vulnerability has been reported in phpESP that could let remote malicious users conduct Cross-Site Scripting or SQL injection. Upgrade to version 1.8-rc1: http://sourceforge.net/projects/phpesp/ There is no exploit code	phpESP Cross-Site Scripting & SQL Injection CVE-2005-3406 CVE-2005-3407	Medium	Secunia, Advisory: SA17333, October 28, 2005

	required.			
PHP-Nuke PHP-Nuke Search Enhanced Module 1.1, 2.0	A vulnerability has been reported in PHP-Nuke Search Enhanced Module that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	PHP-Nuke Cross-Site Scripting CVE-2005-3368	Medium	Secunia, Advisory: SA17296, October 27, 2005
Ringtail CaseBook 6.x	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'login.asp' due to insufficient sanitization of the 'user' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported because different error responses are returned depending on whether or not a valid username is supplied, which could let a remote malicious user obtain sensitive information. The vulnerabilities have reportedly been fixed in version 2005. Currently we are not aware of any exploits for these vulnerabilities.	Ringtail CaseBook Cross-Site Scripting & Information Disclosure CVE-2005-3479 CVE-2005-3480	Medium	Secunia Advisory: SA17383, November 1, 2005
Snitz Communications Snitz Forums 2000, 3.4 .05	A Cross-Site Scripting vulnerability has been reported in 'post.asp' due to insufficient sanitization of the 'type' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Snitz Forum Cross-Site Scripting CVE-2005-3411	Medium	Security Focus, Bugtraq ID: 15241, October 31, 2005

Subdreamer Subdreamer 2.2.1	Multiple vulnerabilities have been reported in Subdreamer that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Subdreamer SQL Injection CVE-2005-3423	Medium	Security Focus, ID: 15238, October 29, 2005
Thomas Rybak MG2 0.5.1	A vulnerability has been reported in MG2 that could let remote malicious users bypass authentication. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	MG2 Authentication Bypassing CVE-2005-3432	Medium	Security Focus, ID: 15235, October 29, 2005
TikiWiki Project TikiWiki 1.9.1, 1.8.5	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of unspecified user-input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/tikiwiki/tikiwiki-1.9.1.1.tar.gz **Gentoo:** **http://security.gentoo.org/glsa/glsa-200510-23.xml** There is no exploit code required.	TikiWiki Unspecified Cross-Site Scripting CVE-2005-3283	Medium	Security Tracker Alert ID: 1015087, October 20, 2005 **Gentoo Linux Security Advisory, GLSA 200510-23, October 28, 2005**
Woltlab Burning Board 2.5	Multiple vulnerabilities have been reported in Woltlab Burning Board Database Module, that could let remote malicious users perform SQL Injection. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this	Woltlab Burning Board SQL Injection CVE-2005-3369	Medium	Secunia Advisory: SA17347, October 27, 2005

	vulnerability.	

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **IPTV Set For Massive Growth Spurt: Survey:** According to a study by Analysis International, IPTV will become the next global growth industry. The China IPTV market, in particular, will skyrocket, reaching 16.7 billion RMB in revenue and nearly 17 million users by 2009. The early stages of market cultivation may pose some threats and risks, the group says. Uncertain regulations, insufficient hardware platforms, an immature value chain and unclear business models are the main concerns right now. Source: http://www.networkingpipeline.com/showArticle.jhtml?articleID=173400478.

Wireless Vulnerabilities

- Nothing significant to report.

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
November 2, 2005	multispoof-0.7.0.tar.gz	N/A	An application that exploits weak, address based authentication that is frequently implemented by ISPs in Ethernet networks.
November 2, 2005	snort_bo_overflow_ win32.pm.txt	Yes	Exploit for the Snort Back Orifice Preprocessor Remote Buffer Overflow vulnerability.
November 2, 2005	up-imapproxy-exp.txt	Yes	Proof of Concept exploit for the Imapproxy Format String vulnerability.
November 2, 2005	vubbXSS.txt	No	Exploit details for the VUBB VUBB Cross-Site Scripting & Path Disclosure vulnerabilities.
November 1, 2005	0510-exploits.tgz	N/A	New Packet Storm exploits for October, 2005.
October 31, 2005	backoffice_mult_exp.pl	No	Proof of Concept exploit for the Comersus BackOffice Multiple Input Validation And Information Disclosure

			vulnerabilities.
October 31, 2005	ethereal_slimp3_bof.py.txt	Yes	A Denial of Service exploit for the SLIMP3 protocol dissector vulnerability.
October 31, 2005	VERITAS-Linux.pl.txt VERITAS-Win32.pl.txt VERITAS-OSX.pl.txt	Yes	Exploits for the VERITAS NetBackup Arbitrary Code Execution vulnerability.
October 31, 2005	XH-Hasbani-HTTPD-DoS.c	No	Script that exploits the Hasbani Web Server Denial of Service vulnerability.
October 30, 2005	cirt-39-advisory.pdf	Yes	Exploitation details for the Novell ZENworks Patch Management SQL Injection vulnerability.
October 30, 2005	MS05-047-DoS.c	Yes	Remote Denial of Service exploit for the Microsoft Windows Plug and Play Arbitrary Code Execution vulnerability.
October 30, 2005	PBLang465.txt	No	Exploitation details for the PBLang Multiple Cross-Site Scripting Vulnerabilities.
October 30, 2005	vCard29.txt	No	Exploitation details for the Belchior Foundry VCard Remote File Include vulnerability.
October 29, 2005	subdreamer_sql.pl	No	Proof of Concept exploit for the Subdreamer Multiple Remote SQL Injection vulnerabilities.
October 27, 2005	advisory-103.txt	No	Proof of Concept exploit for the Techno Dreams Multiple Product SQL Injection vulnerability.
October 27, 2005	flysprayXSS.txt	No	Exploitation details for the Flyspray Multiple Cross-Site Scripting vulnerability.
October 27, 2005	msn-cap.c	N/A	A simple libpcap based MSN protocol sniffer.
October 27, 2005	mybbpr2.pl.txt	No	Proof of Concept exploit script for the MyBulletinBoard SQL Injection vulnerability.
October 27, 2005	nklan.pl	No	Exploit for the Nuked Klan Multiple Cross-Site Scripting & SQL Injection vulnerability.
October 27, 2005	php.4.4.1.txt	Yes	Exploit for the php 4.4.1 .htaccess apache DOS vulnerability.
October 27, 2005	php-iCalendar.txt	No	Exploitation details for the PHP ICalendar Remote File Include vulnerability.

October 27, 2005	phpnuke78sql.txt	No	Proof of Concept exploit for the PHPNuke Multiple Modules SQL Injection Vulnerabilities.
October 27, 2005	saphpLesson.txt	No	Exploit details for the SaphpLesson SQL Injection vulnerability.
October 26, 2005	mwchat.txt	No	Exploit for the MWChat SQL Injection vulnerability.
October 26, 2005	phpBB-IE-gif.txt	Yes	Exploit for the phpBB Cross-Site Scripting vulnerability.
October 26, 2005	UMPNPMGR.c	Yes	Proof of Concept exploit for the Microsoft Windows Plug and Play Arbitrary Code Execution vulnerability.

[back to top]

Trends

- US-CERT is aware of publicly available Proof of Concept code for an Oracle worm. Currently, US-CERT cannot confirm if this code works but they are working with Oracle to determine the threat posed by this code.
- US-CERT is aware of publicly available exploit code for a buffer overflow vulnerability in the Snort Back Orifice preprocessor. This vulnerability may allow a remote, unauthenticated attacker to execute arbitrary code, possibly with root or SYSTEM privileges.
- **Your Next IM Could Be Your Network's Last:** According to data that was collected by IMlogic, the number of instant messaging oriented attacks rose by 30 percent over September when compared to last year. October 2005 counted 1300 percent more threats than the same month in 2004. This will eventually lead to an automated worm that will strike hundreds of thousands of machines in seconds.
  Source: http://www.techweb.com/wire/security/173401244
- **Barrage of Viruses Hits in October:** Sophos reports 1,685 new viruses and variants came out in October. Central Command also reports big numbers for October. There were a record number of viruses that hit the Internet in October but, but none of them were wide-spread and dangerous. Source: http://www.esecurityplanet.com/trends/article.php/3560696.
- **Rootkit-Armed Worm Attacking AIM:** According to FaceTime, a worm spreading through America Online's Instant Messenger (AIM) network carries a dangerous rootkit, code designed to hide a hacker's work from anti-virus scanners. Sdbot.add includes the "lockx.exe" rootkit. Source: http://www.informationweek.com/story/showArticle.jhtml?articleID=172901455**.**
- **Anti-Spyware Group Publishes Guidelines:** The Anti-Spyware Coalition has released guidelines to help consumers assess products designed to combat unwanted programs that sneak onto computers. Source: http://www.washingtonpost.com/wp-dyn/content/article/2005/10/27/AR2005102700819.html.
- **Spammers exploit bird flu fears:** Sophos has reported a large increase in emails that offer online purchases of Tamiflu, the only know medicine that deals with the human version of the avian flu. Source: http://www.itweek.co.uk/vnunet/news/2144878/spammers-bird-flu.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folders.
2	Mytob-BE	Win32 Worm	Increase	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling anti virus, and modifying data.
3	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
4	Mytob-GH	Win32 Worm	New	November 2005	A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender's address.
5	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
6	Netsky-Z	Win32 Worm	Increase	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.
7	Lovgate.w	Win32 Worm	Decrease	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer

					networks. Attempts to access all machines in the local area network.
8	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
9	Zafi-B	Win32 Worm	Decrease	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
10	Mytob.C	Win32 Worm	Decrease	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.

Table Updated November 1, 2005

[back to top]